REMARKS

In the Official Action mailed on **12 July 2006** and the Advisory Action
mailed on **22 August 2006**, the Examiner reviewed claims 1-39. Claims 14-26
were rejected under 35 U.S.C. 112, first paragraph as failing to comply with the
written description requirement. Claims 14-26 were rejected under 35 U.S.C. 101
because the cited computer readable medium includes nonstatutory subject matter.
Claims 1-39 were rejected under 35 U.S.C. 102(e) as being anticipated by Wu et
al. (US Pub. No. 2005/0033726 hereinafter "Wu").

Rejections under 35 U.S.C. §112 first paragraph

Claims 14-26 were rejected as failing to comply with the written
description requirement. Examiner avers that the claimed subject matter is
directed to new matter arising from a deletion of subject matter from the
specification.

Accordingly, Applicant has amended the specification to include the
previously deleted subject matter. No new matter has been added or deleted.

Rejections under 35 U.S.C. §101

Claims 14-26 were rejected for including nonstatutory subject matter.
More specifically, claims 14-26 were rejected for claiming transmission mediums.

Accordingly, Applicant has amended independent claim 14 to limit a
computer-readable storage medium to any device that can store code and/or data
for use by a computer system. This amendment finds support on page 5,
paragraph [0027] of the instant application.

Furthermore, Applicant does not include computer instruction signals
embodied in a transmission medium (with or without a carrier wave upon which
the signals are modulated) as part of the claimed computer-readable storage
medium of claims 14-26.

10

Hence, Applicant respectfully submits that independent claim 14, and claims 15-26, which depend upon claim 14, no longer pertain to nonstatutory subject matter, and thus are in condition for allowance.

Rejections under 35 U.S.C. §102(e)

Independent claims 1, 14, and 27 were rejected as being anticipated by Wu. Applicant respectfully points out that Wu teaches using a metadata view module to abstract and present to a user data from different native data sources (see Wu, page 1, paragraphs [0008]-[0009], see Wu, page 1, paragraph [0012], and see Wu, page 3, paragraph [0042]). Note that Wu is limited to creating a structured summary of data for presentation purposes (see Wu, page 3, paragraph [0040], lines 9-12). Wu does not teach producing data or altering the storage of data (see Wu, page 3, paragraph [0040], lines 5-9). Furthermore, note that Wu's teachings on security are limited to placing restrictions on data views (see Wu, page 3, paragraph [0042], lines 2-5, and see Wu, page 4, paragraph [0053]).

In contrast, the present invention teaches a method for securing and manipulating metadata in a database (see page 3, paragraph [0009], see page 4, paragraph [0010], lines 1-2, and see page 9, paragraph [0037], lines 1-2 of the instant application). Note that manipulating metadata can involve: creating metadata, deleting metadata, and editing metadata (see page 8, paragraph [0036] of the instant application).

Furthermore, the present invention teaches a method to improve security by assigning distinct privileges for manipulating metadata to distinct roles (see page 3, paragraph [0010] of the instant application). For example, a super user can organize metadata into collections, and assign administrators and data stewards to the collections (see page 7, paragraph [0032], lines 15-17, see page 8, paragraph [0034], lines 6-8, and see page 8, paragraph [0035], lines 11-12 of the instant application). Furthermore, an administrator can add metadata to a collection, which the super user has assigned to the administrator; however, the

11

administrator can neither edit nor delete the metadata (see page 8, paragraph [0034], lines 8-10 of the instant application). A data steward can edit and delete the metadata; however, the data steward cannot add the metadata to the collection (see page 8, paragraph [0035], lines 12-14 of the instant application). A user can create metadata; however, if a super user adds the metadata to a collection, the user loses all privileges over the metadata unless the super user gives the user data-steward privileges (see page 8, paragraph [0036] of the instant application).

Hence, the present invention is advantageous because it provides a method for securing metadata without assigning too many privileges, and thus too much trust, to a single user, the super user. Furthermore, the present invention facilitates scaling a metadata warehouse by enforcing a sharing of responsibilities among multiple users.

Examiner avers that Wu teaches differentiating between roles and responsibilities of administrators. Applicant respectfully disagrees. There is nothing in Wu that teaches disseminating privileges among different types of users. Wu does mention different types of users to illustrate the framework taught by Wu for component reuse (see Wu, page 3, paragraph [0037], lines 1-8). However, Wu does not differentiate between the types of privileges of these different types of users; Wu only differentiates between the scale of the privileges (see Wu, page 3, paragraph [0037], lines 8-15).

Furthermore, Examiner avers that a data manager is a data steward. However, Wu never defines the capabilities of a data manager. If a data manager is one who handles, controls, or directs data as Examiner suggests, then there is no distinction between a data manager, and an administrator or super user. However, the present invention, in contrast to Wu, does differentiate between a super user, an administrator, and a data steward. The present invention teaches that a super user is a user who organizes metadata into collections, and controls access to the various collections by assigning the administrators and data stewards to the collections (see page 7, paragraph [0032], lines 15-17, see page 8, paragraph

12

[0034], lines 6-8, and see page 8, paragraph [0035], lines 11-12 of the instant application). An administrator is a user who is responsible for adding metadata to a collection that they have been assigned to administer by the super user (see page 8, paragraph [0034] of the instant application). A data steward is a user that can edit and/or delete metadata that has been placed into a collection by an administrator (see page 8, paragraph [0035] of the instant application). Note that the super user assigns the data steward to this collection. Furthermore, note that a user who creates metadata cannot edit or delete the metadata once an administrator has added it to a collection (see page 8, paragraph [0036], lines 21-26 of the instant application).

Accordingly, Applicant has amended independent claims 1, 14, and 27 to clarify that the present invention teaches manipulating metadata in a collection, wherein only a data steward can manipulate the metadata in the collection, and wherein manipulating the metadata includes editing and deleting the metadata. This amendment finds support on page 8, paragraphs [0035]-[0036] of the instant application. Applicant has cancelled dependent claims 4, 17, and 30 without prejudice.
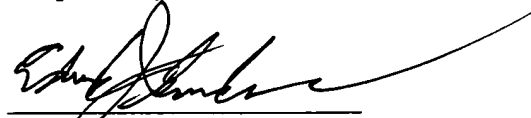
Hence, Applicant respectfully submits that independent claims 1, 14, and 27 as presently amended are in condition for allowance. Applicant also submits that claims 2-3, and 5-13, which depend upon claim 1, claims 15-16, and 18-26, which depend upon claim 14, and claims 28-29, and 31-39, which depend upon claim 27, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By _____
Edward J. Grundler
Registration No. 47,615

Date: 29 August 2006

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1663
FAX: (530) 759-1665
Email: edward@parklegal.com

14